

Key Stage 4: Age 14-16

STAYING SAFE WITH MONEY ONLINE



THE
FAMILY
BUILDING
SOCIETY

Why is it important to protect your money?

People now use digital money more than cash. However, in the same way as cash, with mobile banking apps, online banking and internet shopping our money can still be at risk.

With this guide you can learn to recognise risky money situations and to know how to stay safe in the digital world of money.

When your account allows you to have a debit card, you can make purchases in store and online, and draw out cash from ATM machines. That's why it is so important to know how to protect your money.



What will you learn?

These challenges will help you:

- ✓ Recognise and avoid potentially fraudulent situations around money
- ✓ Explain how to make safe digital money transactions and how to minimise risks
- ✓ Know what steps to take in the event of being a victim of financial fraud or identity theft
- ✓ Understand that it is our responsibility to ensure that financial transactions are secure and to keep our personal information safe.

1 SCAM BUSTER CHALLENGE

Nobody likes to lose money, so even if your money is in a bank account you still need to know how to keep it safe. Just as pickpockets might steal your purse, scammers may try to steal your digital money. This challenge will help you learn to recognise different types of scams and be more alert to potential risks.

Here are some key questions to think about:

- What do you already know about managing and spending money online?
- How might online banking and shopping be useful?
- What do you already know about scams and fraud?
- How many different types of scams and fraud can you think of? e.g. fake emails or bogus competitions.
- How would you be able to recognise a scam?



Use the internet to find out more about the following scams:

Phishing Vishing Smishing

Purchase scams e.g. fake tickets

Identity fraud

Share what you find out with an adult and ask them to share their own knowledge or experiences of online scams.

Which type of scam do you think young people are most likely to fall victim to?

STAYING SAFE WITH MONEY ONLINE

? Did you know?

There are lots of advantages to online shopping:

- Easy to use and access
- You can bank or shop when you want
- Quick to keep track of your money - check your balance, move money from one account to another or pay bills.

But don't forget there can be disadvantages too:

- You must have a bank account that can be accessed online
- You will need access to the internet
- If there's a problem you may have to telephone or use webchat to solve the issue.

! Internet money fraud is big business - in 2019 the banks stopped over £4.5 million of fraud each day.

2 HOW TO MAKE SAFE MONEY TRANSACTIONS

Knowing how to make safe money transactions is really important. Recognising when we're at risk and how to stay safe are key to keeping our money safe online.

Ask an adult in your house to share how they make sure they shop online safely.

How can you apply what you've learnt about the different types of scams and fraud to understand how to make safe money transactions?

Q Why do you think it's important to keep this information safe?

A Fraudsters could try to use your information to impersonate you and get access to your money if you don't keep your information safe.

Q Why shouldn't you use the same password for lots of different accounts?

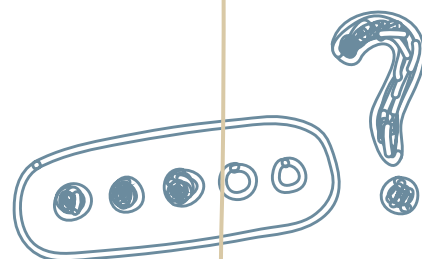
A If scammers or hackers find your password they could access more than one account.

Q How do you create a strong password?

A A strong password is one which does not contain personal information but has upper and lower case letters, numbers and symbols – but is still one you can remember! There's lots of advice on the internet to help you.

Q How can you tell if a website is secure?

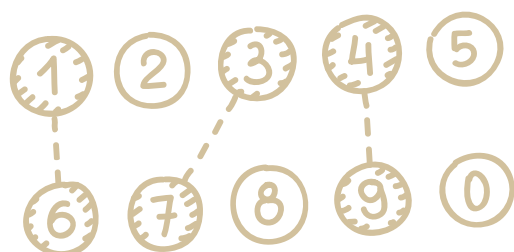
A Look for a closed padlock and a web address beginning with HTTPS rather than HTTP.



? Did you know?

It's our personal responsibility to protect our personal and financial information – so it's down to each of us to do our best!

- Lots of errors occur because of mistyped numbers so always check that the information entered is correct before you click to make a payment.
- Many people never check their bank statement and so don't spot something is wrong until it's too late.
- It's really important not to share your personal information such as passwords and PIN numbers.
- You should always log out from your account once you've finished.



STAYING SAFE WITH MONEY ONLINE



3 KNOW WHAT TO DO IF THINGS GO WRONG

Sometimes, however careful we've been, we might still get scammed or fall victim to financial fraud. This can be scary and stressful, after all no one likes to lose money.

How can you avoid falling victim to fraud and scams?

Q What should you do if you suspect that someone has accessed your PIN?

A If you see a transaction on your account that you don't recognise then you should ring your bank or building society straight away. They can cancel your card and give you new security details.

Q What should you do if you're asked for your bank account details and password?

A Your bank will never ask for your password or full pin number over the phone or by email, however they may ask for memorable information and account details such as your sort code and account number. If you have any doubts about who is requesting the information, don't hand it over.

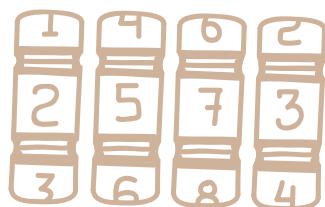
Q What action should you take if you think you have become a victim of financial fraud or a scam?

A You should contact your bank straight away and let them know. Keep a record of all conversations you have with the bank and copies of letters to do with the fraud. The bank will investigate and take action to protect your accounts.

? Did you know?

You can always talk to your bank or building society if you're concerned about keeping your money safe. You could also visit their website to find tips for protecting your money. Remember it's always better to raise concerns and talk to someone you trust for advice.

- It can take time to sort things out and resolve the problem, but the earlier you report a problem the safer your money will be.
- You may also need to contact the police if money has been stolen from your account.
- You can cancel your card and/or request a new PIN at any time.
- Always report an incident, even if you think it's your fault.



BONUS CHALLENGE! RESEARCH

Find and read an article about a real-life financial fraud or scam.

- Talk with an adult or friend about how you might feel if it had happened to you.



Get creative

Make your own video clip about scam busting or staying safe with money online.

One of the most important skills in learning how to manage money is budgeting.

Our guide '**Better budgeting - preparing for independence**' will help you to manage the costs of day-to-day living and prioritise your spending.

Available to download from

familybuildingsociety.co.uk/children-and-money

You might like to check out these websites to learn more about staying safe with money online:

takefive-stopfraud.org.uk

moneyhelper.org.uk

moneysavingexpert.com

moneysupermarket.com



CHECK IT OUT

There's a lot of 'jargon' around digital money and fraud. Get to grips with it here:

Username – a combination of letters and often numbers that identifies a user when logging on to a computer, website or social media platform.

PIN (Personal Identification Number) – a four-digit security number used with cash machines, credit cards and debit cards. It's like an electronic signature that stops anyone else using your account.

Memorable information – this may form part of your log in details on some secure websites alongside your username and password, and is used for additional security.

Identity theft – a type of fraud where someone illegally obtains information about someone else, often for financial gain.

Phishing – a method used by fraudsters to try and gather personal information using deceptive emails and websites.

Smishing (SMS phishing) – a type of fraud where someone tries to trick you into giving them personal or financial information via a text or SMS message.

Vishing (voice phishing) – a type of fraud where someone tries to trick you into giving them personal or financial information over the phone.

Digital wallet – an app that allows you to store all your credit, debit and customer loyalty card details on your phone.

Online banking – allows a user to conduct financial transactions via the internet, also known as internet banking.

Notes

